Math100B - HW #2

Jay Ser

2026.01.18

1.

(a)

$r(1-1) = 0 \iff 1r + (-1)r = 0 \iff r + (-1)r = 0$. So $(-1)r$ is the additive inverse of r, i.e., $-r = -1(r)$.

(b)

Take any $r \in I$. $1 \in R \implies -1 \in R \implies -1 \cdot r = -r \in I$. So ideals are closed under additive inverses. Furthermore, $r - r = 0 \in I$.

(c)

Let $v \in R$ be the multiplicative inverse of u. $u \in I \implies uv = 1 \in I \implies 1r \in I$ for any $r \in R$, i.e., $I = R$.

2.

(a)

Suppose ϕ is injective and take any $x, y \in \ker \phi$. $\phi(x) = \phi(y) = 0 \implies x = y$ by definition of an injection, so $\ker \phi = 0$.

Conversely, suppose $\ker \phi = 0$ and $\phi(x) = \phi(y)$. Then $\phi(x) - \phi(y) = \phi(x - y) = 0 \implies x - y = 0 \implies x = y$. So ϕ is injective.

(b)

Forward direction follows immediately by the definition of a surjection. Conversely, suppose $R' \subset \phi(R)$ and $\exists a_1, a_2, \ldots, a_n \in R$ such that $\phi(a_1) = x_1, \phi(a_2) = x_2, \ldots, \phi(a_n) = x_n$. Every element in $R'[x_1, \ldots, x_n]$, i.e., every multivariate polynomial, is the sum of products of elements of R' and $x_1, \ldots, x_n$. Since ϕ is a homomorphism and each $r \in R$ and $x_1, \ldots, x_n$ have preimages, so do their products and sums. This shows that ϕ is surjective.

(c)

Injection $\Phi|_R = \phi$, so Φ injective $\implies$ ϕ by definition. Vice versa, suppose ϕ is injective and $\Phi(f(x)) = \Phi(g(x))$ in $S[x]$ for some $f(x) = \sum_{k=0}^{n} a_k x^k, g(x) = \sum_{k=0}^{m} b_k x^k \in R[x]$. Namely, suppose f is of degree n and g is of degree m. Using $'$ to denote images under Φ,

$$\Phi(f(x)) = \sum_{k=0}^{n} a'_k x^k, \quad \Phi(g(x)) = \sum_{k=0}^{m} b'_k x^k$$

Because Φ is a homomorphism, $\forall k \leq \min\{n, m\}$, the monomials $a'_k x^k = b'_k x^k$, which implies $a' = b'$ in S. Since ϕ is injective, $a = b$ in R. Finally, suppose $n \neq m$; without loss of generality, suppose $n < m$. Because $\Phi(f(x)) = \Phi(g(x))$ in $S[x]$, $b'_k = 0$ for all $n < k \leq m$. But $b'_k = \Phi(b_k) = \phi(b_k)$, where ϕ is injective; so $b_k = 0$. Namely, $b_m = 0$. This contradicts the fact that g is a polynomial of degree m in $R[x]$. So $m = n$. This shows that f and g have the same degree and the same coefficients, so $f = g$ in $R[x]$; Φ is injective.

Surjection Once again, $\Phi|_R = \phi$. Suppose Φ is surjective. Then every constant in $S[x]$, i.e., $\forall s \in S$, $\exists f(x) \in R[x]$ such that $\Phi(f(x)) = s$. If $f(x) = \sum_{k=0}^{n} a_k x^k$, then $a'_k = 0$ for all $0 < k \leq n$ and $a'_0 = s$. So $\Phi(a'_0) = s$ as well. Namely, a_0 is a constant in $R[x]$, so a_0 can be identified as an element of R. So $\forall s \in S$, $\Phi(r) = \phi(r) = s$ for some $r \in R$. This shows ϕ is surjective.

Conversely, suppose ϕ is surjective and take any $g(x) = \sum_{k=0}^{n} b_k x^k \in S[x]$. Then $\forall 0 \leq k \leq n$, $\exists a_k \in R$ such that $\phi(a_k) = b_k$. If $f(x) := \sum_{k=0}^{n} a_k x^k \in R[x]$, then $\Phi(f(x)) = g(x)$. So Φ is surjective.

3.

(a)

In any $\mathbb{Z}/m\mathbb{Z}$, $\overline{n} \in \mathbb{Z}/m\mathbb{Z}$ is a zerodivisor $\iff$ $\exists na = 0 \mod m$ for some $1 < a < m$. One learns in elementary number theory that such an a exists $\iff$ $(n, m) > 1$. So the only elements of $\mathbb{Z}/m\mathbb{Z}$ which are not zerodivisors are those that are not prime to m.

- In $\mathbb{Z}/4\mathbb{Z}$, the only zerodivisor is 2.
- $\mathbb{Z}/5\mathbb{Z}$ has no zerodivisors because 5 is a prime number.
- In $\mathbb{Z}/6\mathbb{Z}$, the zerodivisors are 2, 3, and 4.

(b)

Suppose $ab = 0$ for some $a, b \neq 0$. If a is a unit, then $\exists u \in R$ such that $au = 1$. By the first equation, $abu = 0u = 0$. By the second equation, $abu = aub = 1b = b$, so $b = 0$. This contradicts the assumption that $b \neq 0$.

Because every nonzero element in a field is a unit, no element in a field is a zerodivisor. Hence a field an integral domain.

(c)

Suppose the characteristic of F is not 0; let n be the smallest positive integer such that $\sum_{i=1}^{n} 1 = 0$. Suppose $n = ab$ for integers $a, b > 1$.

$$(\sum_{i=1}^{a} 1)(\sum_{i=1}^{b} 1) = \sum_{i=1}^{n} 1 = 0$$

where the two factors on the left hand side are both nonzero becuase $a, b < n$ and n is the chracteristic of F. This contradicts the fact that any field is an integral domain.

4.

(a)

$x \mapsto 0$ and $y \mapsto 0$ means every polynomial of degree greater than 0 is in the kernal. Vice versa, a nonzero element in the kernal can't have degree 0 because $\forall p \neq 0 \in \mathbb{R} \subset \mathbb{R}[x, y]$, $p \mapsto p \neq 0 \in \mathbb{R}$. This shows that the nonzero elements of the kernal are exactly the polynomials with degree greater than 0

(b)

Denote $K = \ker \phi$ Let

$$\begin{aligned} f(x) &:= (x - (2 + i))(x - (2 - i)) \\ &= (x - 2)^2 - i^2 \\ &= x^2 - 4x + 5 \end{aligned}$$

Since $i + 2$ is a root of $f(x)$, $(f(x)) \subset K$. Conversely, take $g(x) \in K$. Divide $g(x)$ with remainder by $f(x)$:

$$g(x) = f(x)q(x) + r(x), \quad r(x) = 0 \text{ or } \deg(r) < 2$$

Suppose $r(x) \neq 0$. $g(x), f(x) \in K \implies r(x) \in K$. $r(x)$ is clearly not a nonzero constant since the image of $r(x)$ under ϕ would then just be the constant itself, a real number, which is not zero. But $r(x)$ cannot be linear either; if $r(x) = ax + b$ with $a, b \in \mathbb{R}$, then

$$r(i + 2) = a(i + 2) + b = 0 \implies i = -b/a - 2$$

which contradicts the fact that i is not a real number. So $\deg(r) \geq 2$, which contradicts the definition of r induced by the division algorithm. This shows $r(x) = 0$, i.e., $g(x) \in (f(x)) \implies K \subset (f(x))$.

So $K = (x^2 - 4x + 5)$.

(c)

Denote $K = \ker \phi$. Let

$$\begin{aligned} f(x) &:= (x - (1 + \sqrt{2}))(x - (1 - \sqrt{2})) \\ &= (x - 1)^2 - \sqrt{2}^2 \\ &= x^2 - 2x - 1 \end{aligned}$$

Do the same thing as (b)!!! $q+\sqrt{2}$ is a root of $f(x)$, so $(f(x)) \subset K$. Conversely, $f(x)$ divides any $g(x) \in K$ by basically the same argument as (b) because $f(x)$ is a degree 2 polynomial; $f(x)$ is the irreducible (lowest degree) polynomial with $1+\sqrt{2}$ as a root. So $K = (x^2 - 2x - 1)$.

5.

(a)

Suppose $r^n = 0$. Then

$$(1+r)(\sum_{k=0}^{n}(-1)^k r^k) = \sum_{k=0}^{n}(-1)^k r^k + \sum_{k=0}^{n}(-1)^k r^{k+1} = 1$$

I hope the last equality is clear to the grader hehe...

(b)

If n is any positive integer, let $n := \sum_{i=1}^{n} 1$ in the abstract ring R.

Notice that $1+r = 1+r^{p^m}$ for any power m. This is because

$$(1+r)^p = \sum_{k=0}^{p} \binom{p}{k} r^k = 1 + r^p$$

because p is a zerodivisor in R and, as one learns in elementary number theory, for any prime p, $p \mid \binom{p}{k}$ for any $0 < k < p$. Now, one can induct on m. Assume $1 + r^{p^m} = (1+r^{p^{m-1}}$, where $(1+r^{p^{m-1}})$ is a power of $1+r$; this means $1+r^{p^m}$ is a power of $1+r$ as well. Next, the binomial theorem applies once again to yield $(1+r^{p^m})^p = 1 + (r^{p^m})^p = 1 + r^{p^m+1}$. Namely, this shows $1 + r^{p^m+1}$ is a power of $1+r$.

Suppose r is nilpotent with $r^n = 0$. Let α be the smallest power such that $p^\alpha > n$. Then $1 + r^{p^\alpha} = 1$ is a power of of $1+r$, so $1+r$ is unipotent.

6.

(a)

Take $(a+b), (c+d) \in I + J$, where $a, c \in I$ and $b, d \in I$. Then $(a+b)+(c+d) = (a+c)+(b+d) \in I+J$ since $a+c \in I$ and $b+d \in J$. Next, take any $r \in R$. Then $r(a+b) = ra + rb \in I + J$ since $ra \in I$ and $rb \in J$. This shows $I+J$ is an ideal.

(b)

Take $a, b \in I \cap J$ and $r \in R$. $a+b \in I$ and $a+b \in J$ since I and J are ideals $\implies$ $a+b \in I \cap J$. Similarly, $ra \in I \cap J$, so $I \cap J$ is an ideal.

(c)

Take any $x, y \in IJ$. $x + y$ is just another sum whose summands are a product of an element of I and an element of J, hence $x + y \in IJ$. Take any $r \in R$. By the distributive property, $r(x + y)$ is a sum whose summands are of the form rab with $a \in I$ and $b \in J$. But $ra \in I$ because I is an ideal, so the summand is in IJ, and thus the sum $r(x + y) \in IJ$ as well. This shows IJ is an ideal.

To demonstrate that $S := \{ab \mid a \in I, b \in J\}$ need not be an ideal, consider

$$R := \mathbb{Z}[x, y, z, w], \quad (x, y) \lhd R, \, (z, w) \lhd R$$

Then $xz, yw \in S$, but $xz + yw \notin S$. Suppose not; suppose $\exists ax + by \in I$, $cz + dw \in J$ such that

$$(ax + by)(cz + dw) = xz + yw$$

where $a, b, c, d \in R$. Expanding the left hand side, one gets the following system of equations:

$$ad = 0 \tag{1}$$
$$bc = 0 \tag{2}$$
$$bd = 1 \tag{3}$$
$$ac = 1 \tag{4}$$

(3) and (4) show that a, b, c, d are all units, which contradicts (1) and (2) showing that one of a and d and one of b and c must be 0 (since $\mathbb{Z}$ is an integral domain, $\mathbb{Z}[x, y, z, w]$) is an integral domain)

7.

(a)

Define the substitution homomorphism

$$\varphi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]; \quad \varphi|_{\mathbb{Q}} = \mathrm{id}, \quad x \mapsto \sqrt{2}$$

Denote $K := \ker \varphi$. Then $x^2 - 2 \mapsto 0$, so $(x^2 - 2) \subset K$. Conversely, take any $f(x) \in K$. Divide $f(x)$ with remainder by $x^2 - 2$:

$$f(x) = q(x)f(x) + r(x), \quad r(x) = 0 \text{ or } \deg(r) < 2$$

If $r(x) = 0$, then $f(x) \in (x^2 - 2)$. Suppose $r(x) \neq 0$. Since $f(x)$ and $x^2 - 2$ are both in the ideal K, $r(x) \in K$. Now, $r(x)$ cannot be a constant because $\forall q \in \mathbb{Q}$, $q \mapsto q \neq \sqrt{2}$ since $\sqrt{2}$ is irrational. But $r(x)$ cannot be a linear polynomial either; if $r(x) = ax + b$ with $a, b \in \mathbb{Q}$ and $r(\sqrt{2}) = 0$, then $\sqrt{2} = -b/a \in \mathbb{Q}$, which is a contradiction. So $r(x)$ has degree greater or equal to 2, which contradicts the assumption on $r(x)$ due to the division algorithm. This shows that $r(x) = 0$, which implies $f(x) \in (x^2 - 2)$ always. Thus $K = (x^2 - 2)$, and

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}[\sqrt{2}]$$

by the First Isomorphism Theorem.

(b)

Denote $I := (6, 2x-1)$. Notice that $6x + 3(2x-1) = 3 \in I$, so $I = (3, 6, 2x-1)$. Since $3 \mid 6$, 6 is a redundant generator for I. In other words, $I = (3, 2x-1)$.

First, let $c_3 : \mathbb{Z}[x] \to (\mathbb{Z}/3\mathbb{Z})[x]$ be the reduction homomorphism mod 3. Clearly the elements of the kernal are exactly all the polynomials of $\mathbb{Z}[x]$ such that 3 divides all of the polynomial's coefficients, This means $\ker c_3 = 3\mathbb{Z}[x]$ (the ideal generated by 3 in $\mathbb{Z}[x]$), and it follows $\mathbb{Z}[x]/(3\mathbb{Z}[x]) \cong (\mathbb{Z}/3\mathbb{Z})[x]$ by the First Isomorphism Theorem.

Consider the image of $2x-1$ under c_3, which, using bar notation, is $\overline{2}x - \overline{1}$. Notice that the ideal $(\overline{2}x - \overline{1}) \lhd (\mathbb{Z}/3\mathbb{Z})[x]$ corresponds to $(2x-1, 3) \lhd \mathbb{Z}[x]$, and thus $(\mathbb{Z}/3\mathbb{Z})[x]/(\overline{2}x - \overline{1}) \cong \mathbb{Z}[x]/(3, 2x-1)$ by the Correspondence Theorem. Thus, to identify the latter quotient ring as $\mathbb{Z}/3\mathbb{Z}$, consider the substitution homomorphism

$$\varphi : (\mathbb{Z}/3\mathbb{Z})[x] \to \mathbb{Z}/3\mathbb{Z}; \quad \varphi|_{\mathbb{Z}/3\mathbb{Z}} = \mathrm{id}, \quad x \mapsto \overline{2}$$

$\overline{2}x - \overline{1} \mapsto \overline{2}(\overline{2}) - \overline{1} = \overline{4} - \overline{1} = 0$, so $\overline{2}x - \overline{1} \subset \ker \varphi$. Conversely, suppose $\overline{g}(x) \in \ker \varphi$. Dividing $\overline{g}(x)$ with remainder by $\overline{2}x - \overline{1}$ in $(\mathbb{Z}/3\mathbb{Z})[x]$ yields

$$\overline{g}(x) = (\overline{2}x - \overline{1})\overline{q}(x) + \overline{r}(x), \quad \overline{r}(x) = \overline{0} \text{ or } \overline{r}(x) = c \text{ for } c \neq \overline{0} \in \mathbb{Z}/3\mathbb{Z}$$

Suppose $r(x) \neq 0$. Then $\overline{r}(x) \mapsto \overline{r}(\overline{2}) = c \neq 0$. But $\overline{g}(x), \overline{2}x - \overline{1} \in \ker \varphi \implies \overline{r}(x) = c \neq 0 \in \ker \varphi$, which is a contradiction. So $\overline{r}(x) = 0$, which shows $\ker \varphi = (\overline{2}x - \overline{1})$. By the First Isomorphism Theorem,

$$\mathbb{Z}[x]/(6, 2x-1) = \mathbb{Z}[x]/(3, 2x-1) \cong (\mathbb{Z}/3\mathbb{Z})[x]/(\overline{2}x - \overline{1}) \cong \mathbb{Z}/3\mathbb{Z}$$